**Algebraic cryptanalysis on the AAβ cryptosystem**

ABSTRACT

AAβ cryptosystem is a factorization based public key encryption that uses the modulus of N=p2q. In this paper, we present three types of algebraic analysis upon the AAβ cryptosystem. We begin with the continued fraction's method, then followed by the Coppersmith's techniques which present several potential ways to retrieve the prime factor of p and q from the AAβ public keys or the plain text m from the AAβ ciphertext, respectively. For the third analysis, we analyse the congruence relation in order to solve the AAβequation. Thus, based on such analysis, suggestions are offered as a counter measure on how to secure the AAβ cryptosystem during key generation and encryption process.

**Keyword:** AAβ cryptosystem; Continued fraction; Coppersmiths's the-orem; Congruence relation